

Report Tecnico: Analisi Statica Malware

Sample: AgentTesla.exe

Autore: Studente EPICODE

Data: 2 febbraio 2026

Properties	
Filename:	AgentTesla.exe
MD5:	cce284cab135d9c0a2a64a7caec09107
SHA1:	e4b8f4b6cab18b9748f83e9ffd275ef5276199e
CRC32:	5c6ab96d
SHA-256:	18aab0e981eee9e4ef8e15d4b003b14b3a1b0fb7233fade8ee4b6a22a5abbb9
SHA-512:	c45d021295871447ce60250ff9cbeba2b2a16a23371530da077d6235cf5005f10fa22807
SHA-384:	84a8b33a2814c4c58f84799cb6774e8d04c5e3bfee0e31450e990b88b8f489a05641311
Full Path:	C:\Users\FlareVM\Desktop\Malware\Spyware\AgentTesla.exe
Modified Time:	5/21/2025 4:46:10 PM
Created Time:	2/2/2026 2:50:21 PM
Entry Modified Time:	2/2/2026 2:50:21 PM
File Size:	2,932,642
File Version:	
Product Version:	
Identical:	
Extension:	exe
File Attributes:	
Hash Start Time:	2/2/2026 3:20:10 PM
Hash End Time:	2/2/2026 3:20:10 PM
Hashing Duration:	00:00:00.000
OK	

Obiettivo: Analisi statica, Fingerprinting e Rilevamento Packer

Metodologia: Static Analysis (FlareVM)

Indice

1 Introduzione e Scenario	2
1.1 Obiettivi	2
1.2 Ambiente di Analisi	2
2 Fase 1: Fingerprinting	2
3 Fase 2: Analisi Struttura PE	3
4 Fase 3: Rilevamento Packer	4
5 Fase 4: Analisi Stringhe	5
5.1 Dettagli Stringhe	5
6 Conclusioni	6

1 Introduzione e Scenario

1.1 Obiettivi

L'obiettivo di questa attività è condurre un'analisi statica di base su un campione di malware noto come **Agent Tesla**. L'analisi mira a identificare le caratteristiche del file, ottenere i suoi identificativi univoci (hash), analizzare la struttura dell'eseguibile e individuare eventuali tecniche di offuscamento o packing.

1.2 Ambiente di Analisi

L'analisi è stata condotta in un ambiente isolato e sicuro per prevenire infezioni accidentali:

- **Sistema Operativo:** FlareVM (Windows 10)
- **Tool Utilizzati:** HashMyFiles, PEStudio, Detect It Easy (DiE), Strings.
- **File Analizzato:** AgentTesla.exe

2 Fase 1: Fingerprinting

Il primo passo dell'analisi è stato identificare univocamente il file calcolando le sue impronte digitali (Hash). Questo permette di condividere i risultati con la community di sicurezza e verificare se il file è già noto su piattaforme come VirusTotal.

I valori sono stati estratti utilizzando il tool **HashMyFiles**.

Algoritmo	Hash
MD5	cce284cab135d9c0a2a64a7caec09107
SHA-1	e4b8f4b6cab18b9748f83e9ffd275ef5276199e
SHA-256	18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb...

Tabella 1: Fingerprinting del campione Agent Tesla.

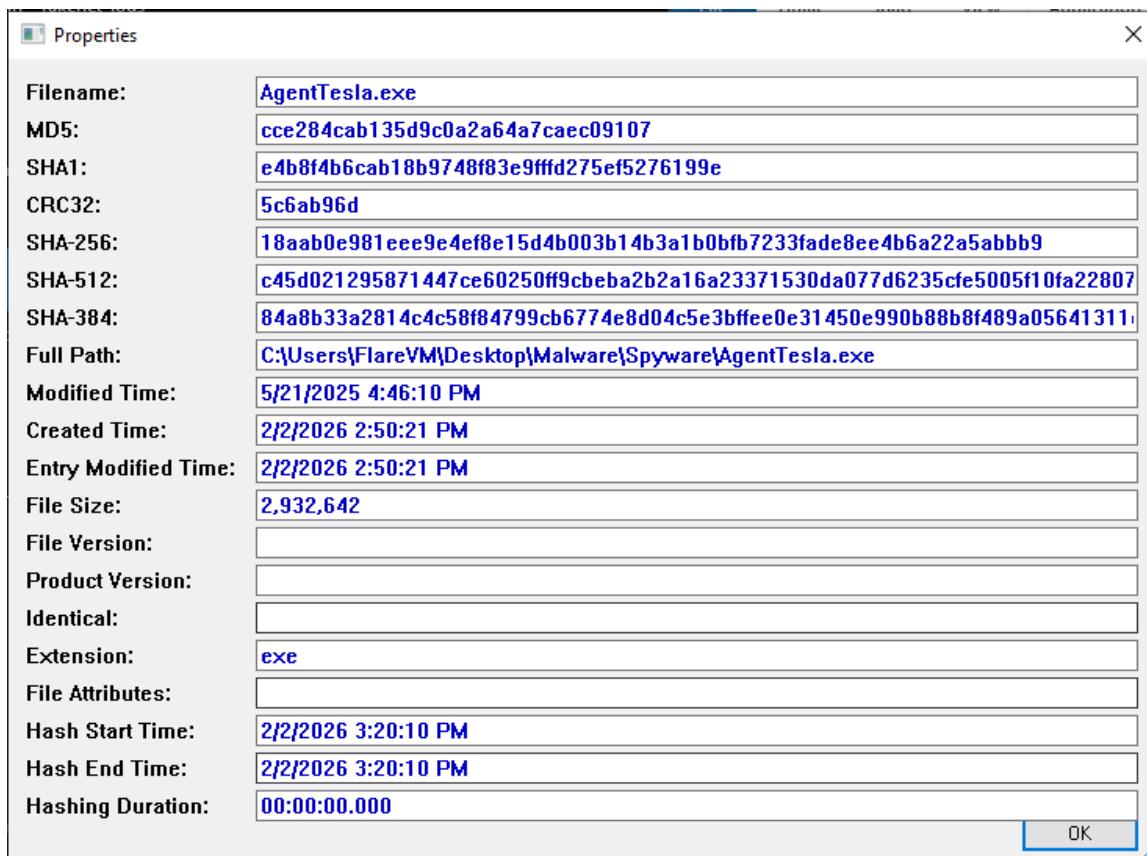


Figura 1: Calcolo degli hash tramite HashMyFiles.

3 Fase 2: Analisi Struttura PE

Utilizzando tool come **Detect It Easy** (DiE), è stata analizzata l'intestazione del Portable Executable (PE) per comprendere l'architettura e la natura del file.

Campo	Valore	Note
Architettura	I386 (32-bit)	Eseguibile a 32 bit.
Timestamp	21/05/2025	Data futura, indicatore sospetto.
Subsystem	GUI	Interfaccia Grafica.
File Type	PE32	Portable Executable

Tabella 2: Struttura del PE.

Dall'analisi emerge una discrepanza significativa tra la dimensione del file su disco (2.80 MB) e la dimensione del PE Header (49.50 KB), suggerendo la presenza di un grande overlay contenente dati compressi.

Property	Value
File Name	C:\Users\FlareVM\Desktop\Malware\Spyware\AgentTesla.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	2.80 MB (2932642 bytes)
PE Size	49.50 KB (50688 bytes)
Created	Monday 02 February 2026, 14.50.21
Modified	Wednesday 21 May 2025, 15.46.10
Accessed	Monday 02 February 2026, 14.56.24
MD5	CCE284CAB135D9C0A2A64A7CAEC09107
SHA-1	E4B8F4B6CAB18B9748F83E9FFFD275EF5276199E

Figura 2: Dettagli del file mostrati da PEStudio/DiE.

4 Fase 3: Rilevamento Packer

L'analisi con **Detect It Easy** (DiE) ha rivelato che il malware non è un semplice eseguibile compilato, ma è un pacchetto di installazione.

- **Packer/Compiler Rilevato:** Nullsoft Scriptable Install System (NSIS) v3.05.
- **Metodo di compressione:** lzma.
- **Linguaggio:** C / Script NSIS.

Questo indica che il vero payload (Agent Tesla) è probabilmente compresso all'interno della sezione di *Overlay* e verrà estratto ed eseguito dall'installer NSIS una volta lanciato.

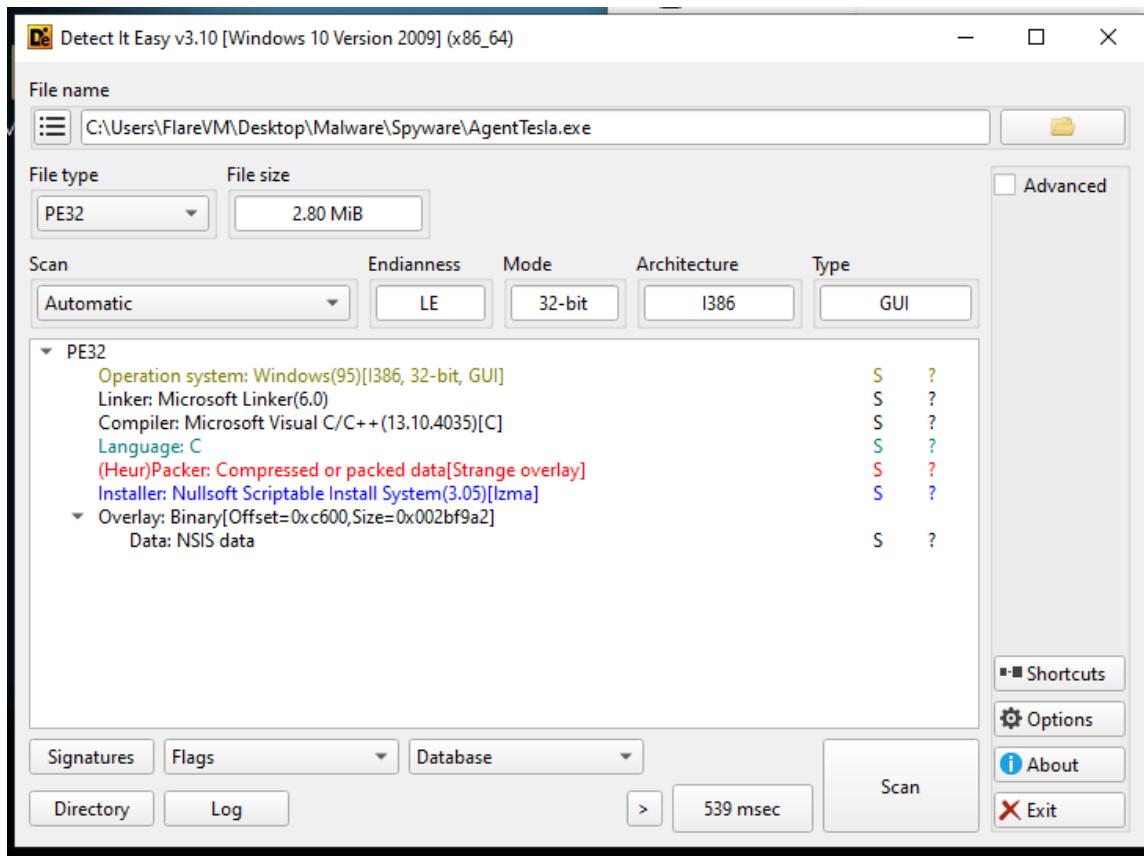


Figura 3: Rilevamento dell'installer NSIS tramite Detect It Easy.

5 Fase 4: Analisi Stringhe

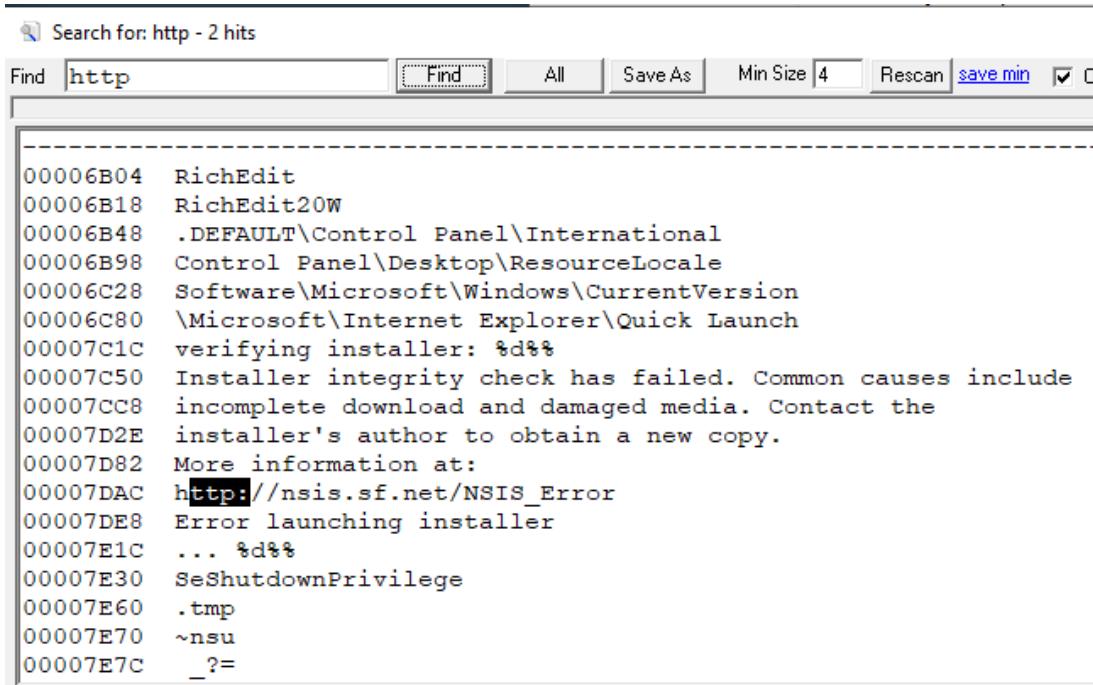
L'estrazione delle stringhe ASCII e Unicode ha permesso di individuare indicatori di compromissione (IOC) e comportamenti previsti, nonostante il packing NSIS.

Categoria	Trovato	Valore
URL/Domini	Sì	http://nsis.sf.net/NSIS_Error (Legittimo NSIS)
Percorsi File	Sì	\Temp (Directory temporanea)
Percorsi File	Sì	\Microsoft\Internet Explorer\Quick Launch
Chiavi Registry	Sì	Software\Microsoft\Windows\CurrentVersion
Privilegi	Sì	SeShutdownPrivilege, requireAdministrator

Tabella 3: Stringhe significative estratte dal binario.

5.1 Dettagli Stringhe

Le stringhe estratte confermano la natura di installer NSIS. Sono presenti riferimenti alla cartella TEMP, dove presumibilmente verrà estratto il payload, e chiavi di registro sotto CurrentVersion, spesso utilizzate per garantire la persistenza (avvio automatico) del malware.



Search for: http - 2 hits

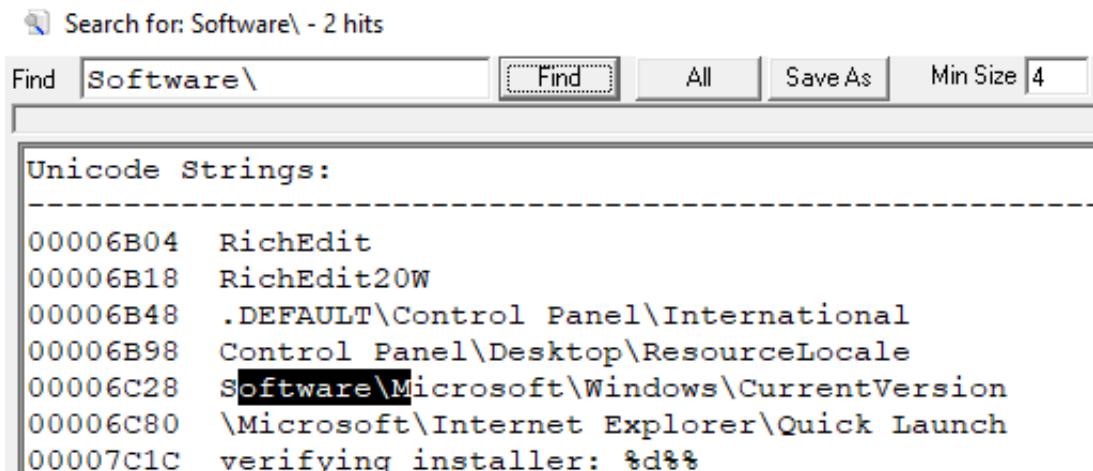
Find http Find All Save As Min Size 4 Rescan save min

```

00006B04  RichEdit
00006B18  RichEdit20W
00006B48  .DEFAULT\Control Panel\International
00006B98  Control Panel\Desktop\ResourceLocale
00006C28  Software\Microsoft\Windows\CurrentVersion
00006C80  \Microsoft\Internet Explorer\Quick Launch
00007C1C  verifying installer: %d%%
00007C50  Installer integrity check has failed. Common causes include
00007CC8  incomplete download and damaged media. Contact the
00007D2E  installer's author to obtain a new copy.
00007D82  More information at:
00007DAC  http://nsis.sf.net/NSIS_Error
00007DE8  Error launching installer
00007E1C  ... %d%%
00007E30  SeShutdownPrivilege
00007E60  .tmp
00007E70  ~nsu
00007E7C  _?=

```

Figura 4: Rilevamento URL NSIS nelle stringhe.



Search for: Software\ - 2 hits

Find Software\ Find All Save As Min Size 4

Unicode Strings:

```

00006B04  RichEdit
00006B18  RichEdit20W
00006B48  .DEFAULT\Control Panel\International
00006B98  Control Panel\Desktop\ResourceLocale
00006C28  Software\Microsoft\Windows\CurrentVersion
00006C80  \Microsoft\Internet Explorer\Quick Launch
00007C1C  verifying installer: %d%%

```

Figura 5: Rilevamento chiavi di registro per possibile persistenza.

6 Conclusioni

L'analisi statica ha permesso di classificare il file **AgentTesla.exe** come un dropper/installer basato su **NSIS**. Il file presenta un timestamp di compilazione sospetto (nel futuro) e contiene un overlay di dati molto grande rispetto all'header PE, confermando che il codice malevolo vero e proprio è compresso all'interno. Le stringhe suggeriscono che il malware tenterà di installarsi nella cartella temporanea e di modificare il registro di sistema per sopravvivere al riavvio.

Per un'analisi completa, sarebbe necessario procedere con l'estrazione del contenuto del pacchetto NSIS o con l'analisi dinamica per osservare il comportamento del payload estratto.